1. **Introdução**
   1. A Norma de segurança da informação **N-SI-002** complementa Política Geral de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação da SOLUS METAL DO BRASIL por seus usuários autorizados.
2. **Propósito**
   1. Estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação da SOLUS METAL DO BRASIL por seus usuários autorizados.
3. **Escopo**
   1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.
4. **Diretrizes**
   1. **Uso de equipamento computacional**
      1. A SOLUS fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais.
      2. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade da SOLUS:
         1. Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade da SOLUS, sendo expressamente proibida a utilização para fins particulares;
         2. A alteração e/ou a manutenção de qualquer equipamento de propriedade da SOLUS é uma atribuição específica do departamento de tecnologia da informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;
         3. Os equipamentos da SOLUS devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;
         4. Computadores de mesa (*desktops*) ou móveis (*notebooks*) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;
         5. A desconexão (*log off*) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;
         6. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;
         7. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com a SOLUS; e
         8. Qualquer dano aos equipamentos da SOLUS será devidamente analisado pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá a SOLUS exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.
      3. A seu critério exclusivo a SOLUS poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção tanto do departamento de tecnologia da informação, quanto da área de segurança da informação de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa;
      4. Não é permitida a conexão de equipamentos particulares na rede administrativa da SOLUS, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento tanto do departamento de tecnologia da informação, quanto da área de segurança da informação.
   2. **Dispositivos de Armazenamento Removível**
      1. A SOLUS poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes:
         1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;
         2. Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos;
         3. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de tecnologia da informação e é obrigatória para todos os equipamentos corporativos; e
         4. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente o departamento de segurança patrimonial para que possam ser tomadas as medidas cabíveis.
   3. **Armazenamento remoto (nuvem)**
      1. A SOLUS disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa;
      2. Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela empresa e homologada pela equipe de segurança da informação da SOLUS.
   4. **Identificação digital**
      1. A SOLUS poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:
         1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.
         2. O usuário deverá informar a equipe de segurança da informação sobre qualquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;
         3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela SOLUS imediatamente revogado;
         4. É de responsabilidade da área de segurança da informação prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.
   5. **Equipamentos de impressão e reprografia**
      1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da SOLUS ou que estejam relacionados com o desempenho das atividades profissionais do usuário.
      2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:
         1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações da SOLUS, classificadas como de uso interno ou confidencial;
         2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;
         3. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pela SOLUS.
   6. **Segurança física**
      1. As instalações de processamento das informações da SOLUS serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.
      2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:
         1. Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;
         2. Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores da SOLUS;
         3. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;
         4. É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis da SOLUS;
         5. É resguardado a SOLUS o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;
         6. É resguardado a SOLUS o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;
         7. Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados organização;
         8. Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.
5. **Papéis e Responsabilidades**
   1. **GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO**
      1. É responsabilidade da Gerência de Segurança da Informação:
         1. Estabelecer e manter atualizados os procedimentos complementares a esta norma;
         2. Comunicar ao CGSI eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.
6. **Sanções e Punições**
   1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.
7. **Revisões**
   1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.
8. **Gestão da Norma**
   1. A norma **N-SI-002** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da SOLUS METAL DO BRASIL.
   2. A presente norma foi aprovada no dia 24/01/2017

|  |  |  |
| --- | --- | --- |
| signaturedimage |  | signaturedimage |
| Albert Solus – Presidente |  | Alfreda SOLUS – Vice-Presidente |